Internet : le conglomérat des réseaux

Laurent Viennot

10 juillet 2006

Qu'est-ce que l'internet ? Littéralement, « internet » vient du néologisme anglais « internetting » qui désigne le fait d'interconnecter des réseaux. L'internet est donc un réseau de réseaux. Comment ça marche ? L'information circule sous forme de paquets acheminés indépendamment les uns des autres. Pour cela, chaque paquet contient un identifiant de la destination : son adresse IP. La manière d'allouer les adresses IP et la manière d'acheminer les paquets sont intimement liées, c'est ce qui permet de faire fonctionner de concert plusieurs centaines de milliers de réseaux connectant ainsi plusieurs centaines de millions de machines entre elles. Cet article vise principalement à donner une idée des principes de base du fonctionnement de l'internet.

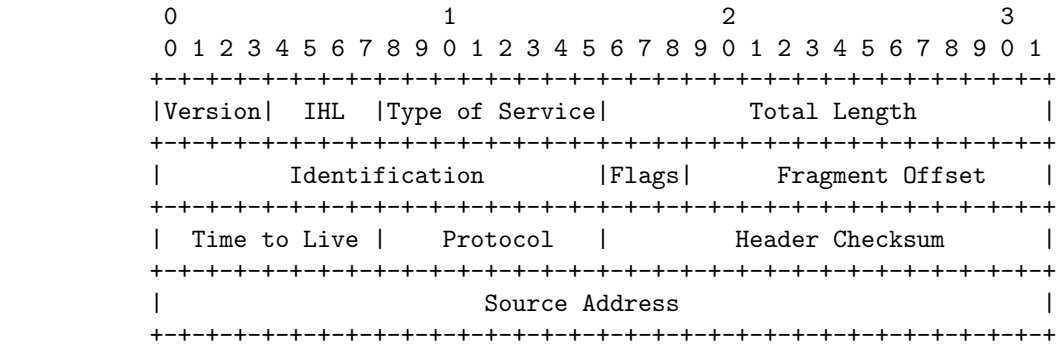
Note pour l'édition : les parties en petits caractères comme ceci sont à considérer pour des rajouts sous forme de pop-up ou bien listent quelques informations de travail dont il conviendra de sélectionner une partie. Les paragraphes 6 à 13 sont aussi candidats à pop-up ou disparition totale. Les commentaires à ce sujet sont les bienvenus.

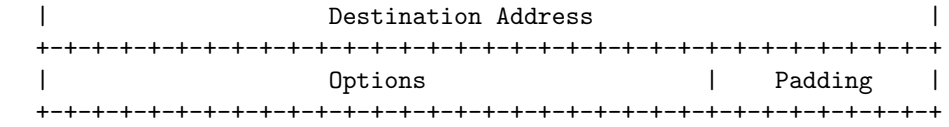
1 Ce qui circule : des paquets

Dans un réseau, l'information qui circule est découpée en unités élémentaire appelées *paquets*. Il s'agit d'une suite suffisamment courte d'octets pour pouvoir être communiquée sous forme numérique et sans erreur sur un câble de communication ou tout autre type de liaison numérique (radio par exemple).

Dans le cas de l'internet, le format des paquets est spécifié par l'Internet Protocol, connu sous l'acronyme IP. On parle donc de paquets IP. Quand on récupère un fichier par exemple, son contenu est découpé en petits morceaux inclus dans une multitude de paquets IP qui vont transiter sur le réseau. Chaque paquet circule indépendamment des autres. Pour cela, il contient un *en-tête* indiquant entre autres quelle est la destination du paquet. Le protocole IP spécifie que cette destination est identifiée par une suite de 4 octets : son *adresse* IP (chaque octet est généralement lu comme un nombre entre 0 et 255).

Voici le format de l'en-tête d'un paquet IP tel que spécifié au bit près dans le standard `http://www.ietf.org/rfc/rfc791.txt` RFC 791 définit par l'`http://www.ietf.org/` IETF (pour « Internet Engeneering Task Force »), l'organisme de standardisation de l'internet. La première ligne indique la signification des quatre premiers octets du paquet (soit 32 bits), la deuxième, celle des quatre suivants et ainsi de suite. Le reste du paquet est constitué par les données qui transitent dans le paquet (typiquement de l'ordre de 1000 octets).





On voit qu'outre l'adresse IP de la destination (cinquième ligne), un paquet IP contient aussi celle de la source (quatrième ligne) et bien d'autres champs comme la version du protocole (quatre premiers bits de la première ligne). La version présentée ici (la plus courante à l'heure actuelle) est la version 4 (IPv4). (Tout paquet IPv4 commence par les bits `0100` soit 4 en binaire.) Le reste des champs sont décrits ci-dessous.

- `Version` indique le type de protocole internet utilisé (4 ou 6 à l'heure actuelle).
- `IHL` indique la longueur de l'en-tête (20 octets en général, qui peuvent être suivis de champs optionnels).
- `Type of Service` permet d'indiquer le type de trafic dont le paquet fait partie (voix, vidéo, transfert de fichier,...). Il peut être utilisé pour demander différentes priorités de service (comme un temps de transit de paquets court, ou un débit maximum, ou une fiabilité maximale). Ce type de traitement évolué des paquets n'existe pas encore à l'échelle de l'internet, mais le format des paquets anticipe sur le futur.
- `Total Length` désigne la longueur totale du paquet.
- `Identification` est un numéro d'identification du paquet (ce numéro est incrémenté à chaque envoi de paquet). Il permet de plus de ré-assembler les fragments d'un paquet trop long pour transiter un seul morceau sur le réseau. `Flags` indique si le paquet a été fragmenté et `Fragment Offset` indique alors la position du fragment transporté par le présent paquet dans le paquet originel.
- `Time to Live` indique un nombre maximal de retransmissions par les routeurs du réseau. Il s'agit d'une sorte de temps de vie car ce champs est décrémenté à chaque retransmission par un routeur et le paquet disparaît du réseau si ce champs atteint zéro. Ce garde fou permet d'éviter qu'un paquet ne circule à l'infini dans le réseau.
- `Protocol` indique le protocole de transfert, c'est-à-dire la manière dont le flot de paquets dont ce paquet fait partie est utilisé. Une en-tête pour le protocole suit généralement l'en-tête IP dans le paquet. Le protocole de transfert le plus utilisé est TCP (pour « Transfert Control Protocol ») qui permet de faire transiter de manière fiable un flot de données (comme un fichier, un mail, une page web, une conversion de tchat,...). Un autre protocole plus rarement utilisé est UDP (pour « User Datagram Protocol ») qui sert à envoyer individuellement des paquets (ou datagrammes) et est utilisé typiquement dans les applications à contraintes temporelles comme la voix sur IP. Mentionnons enfin le protocole ICMP (pour « Internet Control Message Protocol ») qui sert à tester l'état du réseau (il est par exemple utilisé par la commande `ping` qui teste si les paquets arrivent bien à destination d'une adresse).
- `Header Checksum` est une somme calculée sur l'en-tête vue comme une suite de nombres de 16 bits, sa valeur est ajustée de sorte que la somme des nombres fasse zéro. Cela permet de tester assez sûrement qu'aucune erreur de transmission ne s'est glissée dans l'en-tête. Un paquet dont l'en-tête ne passe pas ce test est ignoré.
- `Options` désigne une suite de longueur variable d'octets permettant d'inclure des informations facultatives comme des étiquettes de temps, ou des adresses de routeurs à traverser. Elles sont généralement inutilisées dans les trafics courants.
- `Padding` indique que des octets doivent être rajoutés pour que la longueur de l'en-tête soit toujours un multiple de 4 octets.

2 À l'intérieur d'un réseau

Un réseau est constitué de routeurs et de liens de communication. Un *routeur* est une sorte d'aiguilleur qui possède des *liens* avec d'autres routeurs. Chaque lien est branché au routeur via une *interface*. La principale activité d'un routeur consiste à *router* des paquets :

Routage

1. Un paquet arrive sur une interface,
2. son *en-tête* est lue (et éventuellement modifiée),
3. il est retransmis sur une autre interface.

Le choix de l'interface de sortie dépend de l'en-tête du paquet. Pour faire ce choix, un routeur maintient à jour une *table de routage* qui contient pour une destination donnée le numéro d'interface où faire suivre le paquet. Un *protocole de routage* spécifie les informations que s'échangent les routeurs pour pouvoir construire leurs tables de routage.

Mathématiquement, un réseau se modélise par un graphe dont les nœuds sont les routeurs et les arêtes sont les liens. Trouver comment acheminer un paquet d'un routeur à un autre revient à calculer un chemin dans ce graphe, c'est à dire une suite de routeurs telle que chaque routeur est connecté au suivant.

Ainsi, pour une destination donnée, chaque table de routage doit indiquer à qui faire suivre le paquet (en indiquant l'interface attachée au lien vers celui-ci). Pour une destination donnée, cette relation entre routeur et routeur suivant peut se représenter par un arc d'un routeur vers le suivant. Idéalement, l'ensemble de ces arcs forme un arbre de plus courts chemins enraciné à la destination.

La bête noire du routage est la *boucle*, c'est-à-dire une incohérence dans les tables de routage qui fait qu'un paquet peut se mettre à faire une boucle. Si jamais cela arrive, les liens de la boucle peuvent vite être engorgés par les paquets qui vont se mettre à y circuler indéfiniment. Pour éviter qu'un tel dysfonctionnement ne devienne dramatique, le protocole IP prévoit un champ TTL (pour « Time To Live ») dans l'en-tête des paquets. Quand un paquet est reçu, le champ TTL est décrémenté de 1. Si le TTL atteint 0, le paquet est interdit de retransmission. Ainsi, un paquet ne peut pas circuler indéfiniment dans le réseau.

Toute machine reliée à un des routeurs du réseau peut ainsi communiquer avec tout autre machine reliée à un routeur du réseau. Les machines qui sont ainsi mise en relation par un réseau sont appelées des *hôtes*.

À l'opposé, dans les réseaux téléphoniques (qui existent depuis beaucoup plus longtemps que l'internet), tous les paquets d'une communication se suivent avec régularité sur la même route.

Toute communication commence par l'établissement d'une connexion qui va configurer les éléments du réseau de sorte qu'une route soit réservée pour la suite de paquets qui va suivre. Ces réseaux dédiés à une application donnée comme le transport de la voix n'ont pas la malléabilité de l'internet dont le principe de base consiste à interconnecter tout ce qui peut transporter un paquet IP. On oppose ainsi les réseaux en *mode connecté* comme les réseaux téléphoniques aux réseaux à *commutation de paquets* comme l'internet.

3 Comment agréger les réseaux

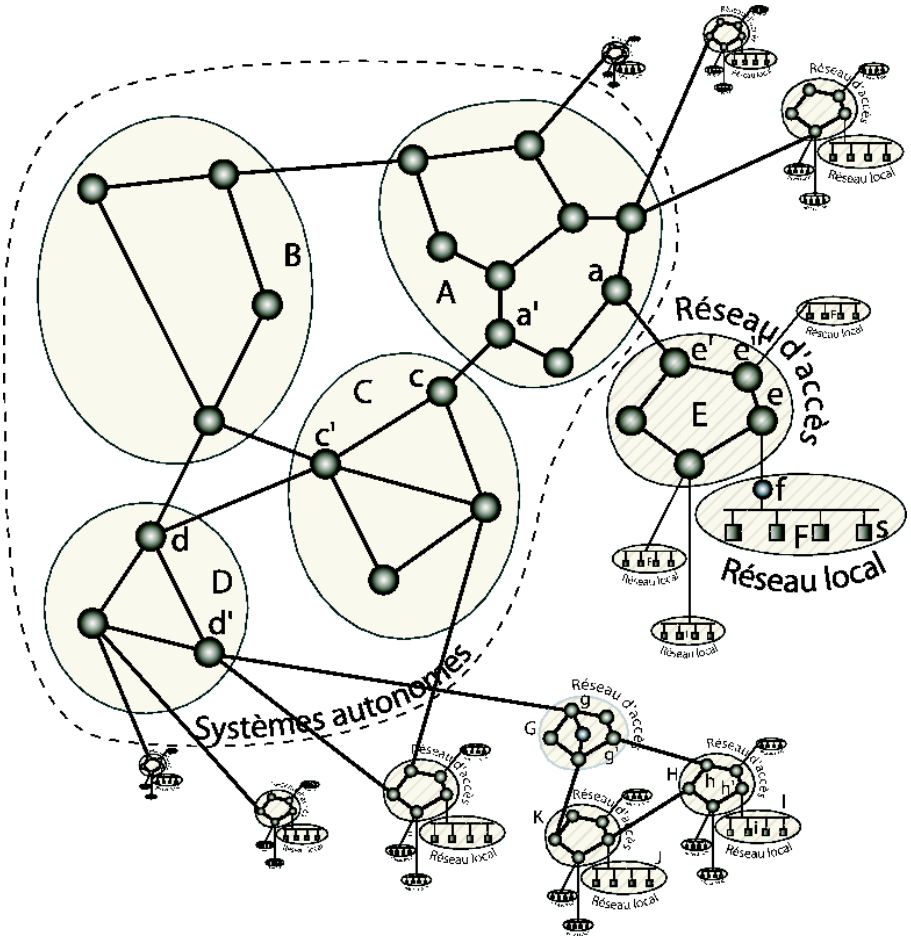
Les hôtes sont les machines des utilisateurs de l'internet, généralement reliés à un réseau local pour lequel un routeur appelé *passerelle* relie le réseau local avec l'internet. La seule décision de routage prise par un hôte est d'envoyer un paquet directement à la destination si elle se trouve dans le réseau local ou à la passerelle sinon.

Tous les routeurs d'un réseau sont gérés par la même organisation et sont reliés entre eux de manière connexe. Certains des routeurs du réseau peuvent avoir des liens vers des routeurs d'autres réseaux, appelons-les des *routeurs de frontière* (pour « border gateway » en anglais). Le monde des destinations, vu d'un routeur de l'internet, se sépare donc en deux populations, celles qui sont accessibles sans sortir du réseau et celle qui sont en dehors du réseau.

Internet est constitué par un empilement hiérarchique de réseaux. Les réseaux du bas de la hiérarchie ne possèdent souvent qu'un seul routeur frontière relié à un réseau de niveau supérieur. Tout paquet pour une destination hors de portée du réseau sera envoyé vers ce lien. On parle de route par défaut puisque les paquets sont envoyés par là si aucune information concernant la destination n'est trouvée dans la table de routage. Elle ne contient en effet que des entrées concernant les destinations accessibles via le réseau. À l'inverse, un routeur du réseau supérieur qui connecte ce réseau à l'internet doit connaître l'ensemble des destinations accessibles via celui-ci au cas où il recevrait un paquet pour l'une d'elles.

Les réseaux de plus haut niveau n'ont pas de route par défaut, on les appelle les systèmes autonomes ou AS (pour « Autonomous System ») et ils constituent la nervure centrale (« backbone ») de l'internet. Les réseaux de différentes organisations sont reliés entre eux au gré d'accords bilatéraux (ou même multi-latéraux). Les deux organisations s'accordent sur les informations que s'échangent les routeurs et sur les conditions commerciales dans lesquelles ils s'échangent du trafic.

Les réseaux intermédiaires de la hiérarchie que nous appellerons *réseau d'accès* (ou « stub network » en anglais) peuvent aussi conclure de tels accords de « peering » à leur niveau. La figure ci-dessous illustre ainsi schématiquement la structure de l'internet.



Le réseau F est par exemple connecté par sa passerelle au réseau E qui est lui-même un sous-réseau du système autonome A. Le réseau F pourrait par exemple être le réseau Wifi d'un particulier dont le modem ADSL f (qui fait aussi routeur Wifi) est relié à un routeur e (au nom de DSLAM) de son fournisseur d'accès à Internet. Ce routeur e fait partie du réseau national E de son fournisseur qui possède une connexion directe avec un système autonome internationalement connecté.

Un réseau local peut aussi être directement connecté à un routeur du réseau d'accès. C'est souvent le cas pour les réseau universitaires ou les réseaux d'entreprise.

Les routeurs des systèmes autonomes possèdent des sortes de méta-tables de routage qui indiquent pour une adresse IP comment atteindre le système autonome où se trouve la destination possédant cette adresse. Plus précisément, chacun de ces routeurs connaît la suite de systèmes autonomes qu'il va falloir traverser pour atteindre la destination. Pour cela, tout routeur frontière connecté au routeur frontière d'un autre système autonome échange avec lui des informations sur les adresses IP gérées par tel ou tel système autonome et sur les interconnexions entre système autonomes selon le protocole de routage BGP (pour « Border Gateway Protocol »).

L'acheminement d'un paquet IP se fait donc généralement ainsi :

Routage dans l'internet

1. le paquet remonte la hiérarchie de réseau jusqu'à un routeur du système autonome de la source,
2. il transite ensuite de système autonome en système autonome jusqu'à celui de la destination,
3. il descend la hiérarchie jusqu'à la passerelle en charge du réseau local de la destination,
4. cette passerelle l'envoie à la destination.

Imaginons par exemple que le nœud s du réseau F envoie un paquet à destination de i (dans le réseau I en bas à droite de la figure ci-dessus). i ne faisant pas partie du réseau F, le routeur Wifi f relaye ce paquet vers sa passerelle par défaut e. e détectant que i n'est pas accessible sous le réseau E le fait parvenir à sa passerelle par défaut e' (le protocole de routage interne au réseau E indique qu'il faut passer par e'' pour cela). e' passe alors le paquet à a dans le réseau A. Le réseau A ne possède pas de passerelle par défaut (il s'agit d'un système autonome). Ses routeurs savent que i est accessible sous le système autnonome D qu'ils peuvent atteindre via C qui est accessible via le routeur a' de A. a fait ainsi parvenir le paquet à a' (par routage interne à A) qui passe à c qui passe de manière similaire à c' qui relaye le paquet vers d. d sait que i est dans un sous-réseau de D accessible via d' à qui il passe donc le paquet. d' qui interconnecte G sait qu'il doit passer le paquet à ce réseau d'accès intermédiaire pour atteindre i, le paquet circule ainsi ensuite par g, g', h, h' pour arriver finalement à i.

Bien sûr, un réseau intermédiaire de la hiérarchie peut s'apercevoir que la destination se trouve dans un autre des sous-réseaux qu'il connecte à l'internet auquel cas le paquet redescendra directement vers la destination sans passer par les routeurs de plus haut niveau des systèmes autonomes. De même, un lien de « peering » avec un réseau intermédiaire en charge du réseau de la destination peut permettre de court-cicuiter le passage par les systèmes autonomes.

Par exemple, un paquet envoyé depuis le réseau J à destination de i transitera par K qui utilisera son lien de « peering » vers H qui fera suivre directement vers I à destination de i.

Il est possible d'afficher la suite de routeurs traversés pour atteindre une destination grâce à la commande `traceroute`. Cette commande consiste à envoyer des paquets de `TTL` 1, puis 2, puis 3,... ainsi chaque routeur intermédiaire voit à son tour le `TTL` atteindre 0 et répond par un paquet `ICMP` pour signifier que la destination est inaccessible. Ce paquet contient l'adresse IP du routeur qui permet de l'identifier. Par exemple, depuis une machine de l'INRIA Rocquencourt, la commande `traceroute www.gouv.fr` donne :

```
traceroute: Warning: www.gouv.fr has multiple addresses; using 193.51.224.6
traceroute to a331.g.akamai.net (193.51.224.6), 30 hops max, 38 byte packets
 1  rocq-gw (128.93.1.100)  1.887 ms  1.459 ms  2.501 ms
 2  rocq-royal-gw (192.93.1.106)  3.470 ms  8.980 ms  4.477 ms
 3  193.48.202.1 (193.48.202.1)  2.992 ms  2.966 ms  3.489 ms
 4  193.48.202.122 (193.48.202.122)  3.992 ms  3.988 ms  3.987 ms
 5  193.48.202.132 (193.48.202.132)  2.991 ms  2.989 ms  3.986 ms
 6  inria-g3-2-800.cssi.renater.fr (193.51.182.74)  2.996 ms  3.474 ms  3.489 ms
 7  nri-a-g13-0-20.cssi.renater.fr (193.51.180.173)  3.987 ms  3.480 ms  3.995 ms
 8  nri-a-g1-0-0-101.cssi.renater.fr (193.51.187.17)  5.487 ms  4.460 ms  3.491 ms
 9  193.51.224.6 (193.51.224.6)  5.496 ms  4.972 ms  4.989 ms
```

On voit ainsi que `www.gouv.fr` est un site géré par la société `akamai` qui possède plusieurs miroirs du site. L'adresse cible choisie est accessible via 8 routeurs intermédiaires (notamment des routeurs du réseau `renater` qui est le réseau académique français). À l'inverse, un textttttraceroute vers `www-rocq.inria.fr` donne la route très courte suivante (un simple passage par le routeur du site qui possède deux réseaux) :

```
traceroute to www-rocq.inria.fr (192.93.2.1), 30 hops max, 38 byte packets
 1  rocq-gw (128.93.1.100)  4.202 ms  1.530 ms  2.211 ms
 2  www-rocq1 (192.93.2.1)  2.314 ms  4.318 ms  4.701 ms
```

4 Comment agréger les adresses

La gestion des tables de routage est un élément critique d'un routeur. Son interrogation doit être extrêmement optimisée. Un routeur avec des liens à 1Gbits/sec doit en effet interroger sa table de routage près de un million de fois par seconde puisque chaque lien peut lui apporter plus d'un million de paquets par seconde. Il va de soit que si cette table possédait trop d'entrées, de tels débits ne seraient pas possibles. Les routeurs de plus haut niveau de l'internet arrivent à fonctionner parce que leur tables de routage ne contiennent « que » quelques centaines de milliers d'entrées.

Comment arrivent ils alors à acheminer des paquets vers des centaines de millions d'hôtes ? La clé réside dans l'agrégation des adresses. Une adresse IP est constituée par n'importe quelle suite de 32 bits (soit 4 octets ou encore 4 nombres entre 0 et 255). L'attribution des adresses se fait en regroupant autant que faire se peut les adresses accessibles via une passerelle sous le même préfixe. De même tout réseau de la hiérarchie tentera de représenter l'ensemble des adresses IP qu'il connecte à l'internet par un petit nombre de préfixes. L'annonce de ces seuls préfixes suffit alors à représenter l'ensemble des adresses accessible via ce réseau. Idéalement, toutes les adresses joignables via un système autonome donné devraient pouvoir être identifiées par un même préfixe commun, des préfixes plus longs servant alors à identifier les adresses accessibles par les réseaux d'accès que ce système autonome connecte.

En pratique, les plages d'adresses sont possédées par différentes organisations qui se connectent via tel ou tel système autonome au gré de la conjecture économique. Une telle agrégation idéale

est donc impossible. Notons cependant, que début 2006, les 22 000 systèmes autonomes actuels s'annoncent les uns les autres 180 000 préfixes, ce qui représente une moyenne de 9 préfixes par système autonome, un taux d'agrégation suffisant pour rendre le fonctionnement de l'internet possible et interconnecter entre-eux près de 400 millions d'hôtes.

Cette agrégation par préfixe se traduit en pratique par l'utilisation d'un masque (comme `255.255.0.0` par exemple) qui est une adresse IP fictive constituée d'une suite de 1 suivie d'une suite 0 (255 s'écrit en binaire 11111111). Associé à une adresse IP (par exemple `128.93.0.0`) cela permet d'identifier l'ensemble des adresses de même préfixe qui coïncident sur tous les 1 du masque (celles dont les deux premiers octets sont `128.93` par exemple). Un sous réseau peut alors être construit en regroupant toutes les adresses possédant un préfixe plus long, par exemple toutes celles identiques à `128.93.17.8` pour le masque `255.255.255.0`

5 Comment construire les tables de routage

Que ce soit à l'intérieur d'un réseau où entre les systèmes autonomes, il existe principalement deux types de protocoles de routage permettant de maintenir à jour les tables de routage :

- le routage par vecteur de distances (« distance vector » en anglais),
- le routage par état de liens (« link state » en anglais).

Le routage par vecteur de distances consiste à donner à ses routeurs voisins le vecteur des distances estimées avec toutes les destinations. Il repose sur une version asynchrone de l'algorithme de calcul de plus courts chemins connu sous les noms de Bellman-Ford. Le protocole BGP repose sur le même principe en diffusant plutôt un vecteur de chemins indiquant pour chaque destination la suite de systèmes autonomes qui mène à elle.

Le routage par état de liens consiste pour chaque routeur à diffuser la liste des routeurs avec lesquels il est connecté. Chaque routeur connaît ainsi la topologie complète du réseau et calcule des plus courts chemin selon l'algorithme de Dijkstra.

6 TCP

Un aspect important des réseaux à commutation de paquets est la nécessité de stocker les paquets temporairement dans chaque routeur. En effet, plusieurs paquets peuvent arriver de différents liens pour être retransmis sur le même lien de sortie. Les derniers arrivés doivent donc être stockés le temps de transmettre les premiers. Des tampons permettent ainsi de résister à un pic d'arrivée de paquets pour chaque lien. Si jamais un paquet supplémentaire arrive alors que le tampon est plein, le routeur n'a d'autre choix que de « jeter » le paquet (il ne sera jamais retransmis, il est perdu).

En cas de trafic trop important pour la capacité des liens, l'engorgement dans les tampons des routeurs est inévitable. L'un des piliers algorithmique de l'internet est donc le mécanisme qui permet de limiter le trafic de chaque connexion. C'est le rôle de TCP (pour « Transfer Control Protocol ») de ralentir l'émission de paquets de toute source de trafic dès que celle-ci détecte le moindre signe d'engorgement dans l'acheminement vers ou depuis la destination. TCP s'occupe de plus de retransmettre les paquets perdus. Pour cela, la destination informe la source des paquets qu'elle a bien reçu par acquittements. Si un acquittement manque ou tarde à arriver, la source prend deux décisions : réduire son trafic car il s'agit d'un signe de congestion dans le réseau, et retransmettre le paquet perdu.

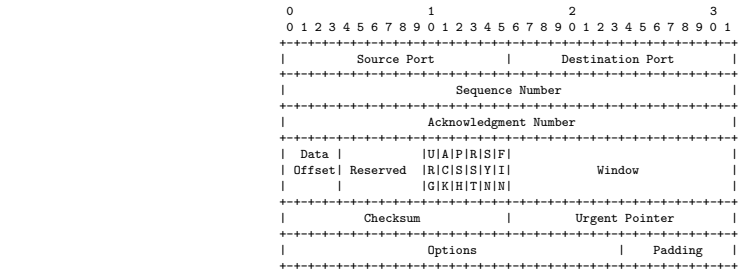
lien vers l'article de François Baccelli

Mentionnons aussi un autre rôle fondamental de TCP : remettre les paquets dans l'ordre. Dans un réseau à commutation de paquet, ill se peut en effet qu'un paquet transite plus vite qu'un autre induisant ainsi une arrivée désordonnée des paquets. Pour permettre la transmission fiable de données, TCP permet ainsi de retrouver l'ordre correct d'émission des paquets.

TCP permet donc l'établissement de sortes de connexions de transmission de données via l'acheminement de datagrammes dans un réseau à commutation de paquets. Pour identifier ces connexions, TCP utilise des ports qui sont des numéros de 2 octets identifiant la connexion pour

la source et la destination. Pour une machine donnée, il y a un seul programme en charge des paquets arrivant sur un port donné (ce programme peut néanmoins gérer plusieurs connexions sur ce port, chaque connexion étant différenciée par l'adresse IP et le port de l'autre participant). Le numéro de port sert ainsi d'aiguilleur pour permettre à une même machine d'accepter plusieurs connexions TCP en parallèle. Les applications les plus courantes de l'internet ont des numéros de port réservés, ainsi le téléchargement de page web auprès d'un serveur web se fait généralement sur le port 80, les serveurs de mail utilisent le port 25,...

Dans un paquet TCP, une en-tête TCP suit immédiatement l'en-tête IP. Son format (d'après le `http://www.ietf.org/rfc/rfc793.txt` RFC 793) est le suivant :



Le port source (respectivement destination) permet d'identifier sur la machine source (respectivement destination) le programme en charge du traitement de l'envoi et du traitement des paquets. TCP est conçu pour un échange symétrique ainsi chaque envoi de la part de la source sert aussi à acquitter un paquet envoyé en sens inverse par la destination. `Sequence Number` est un numéro permettant d'identifier le paquet envoyé. `Acknowledgment Number` indique le numéro du dernier paquet reçu en sens inverse. Les bits `SYN` et `FIN` servent à initier et terminer la connexion respectivement.

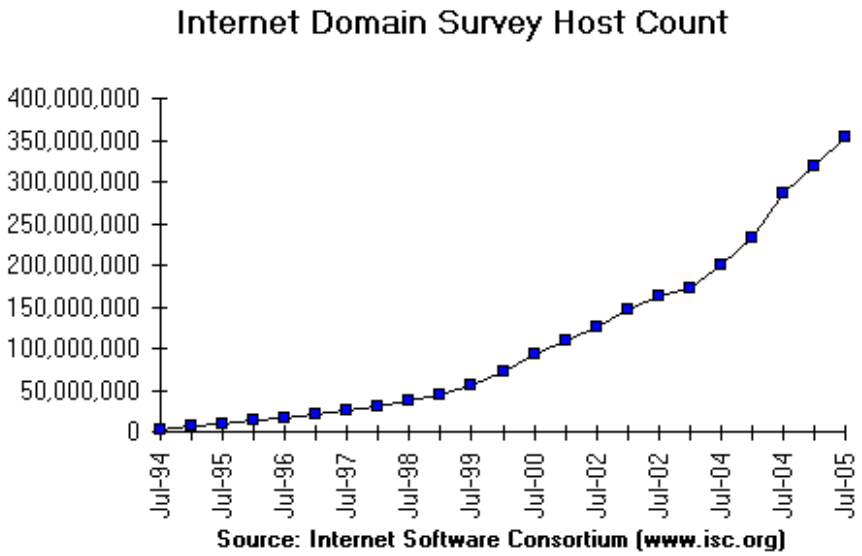
7 Bref historique

On fait souvent remonter la naissance de l'internet à celle de son premier réseau l'ARPANET en 1969. En fait, les premières interconnexions effectives de réseaux remontent à 1983 avec la séparation de l'ARPANET en deux réseaux et sa liaison avec le réseau académique américain CSNET. L'invention d'IP qui permet d'interconnecter des réseaux est généralement attribuée aux américains Vinton Cerf et Robert Kahn à la fin des années 1970. Cependant il serait sans doute légitime de leur voir associer le nom du français `http://www.admi.net/cgi-bin/wiki?LouisPouzin` Louis Pouzin qu'ils ont visité en 1972 et dont les travaux pour le réseau Cyclade les ont sans doute largement inspirés dans la conception d'IP.

Le réseau Cyclades (projet inspiré d'ARPANET et développé à l'IRIA) possédait dès le début des années 1970 une conception centrée sur la commutation de paquets (appelés datagrammes) avec une partie très similaire à IP.

8 Taille

Plus que le nombre d'ordinateurs connectés par l'internet (estimé entre 350 et 400 millions début 2006), il convient de s'intéresser au nombre de réseaux connectés (plus de 180 000, dont seulement 22 000 assurent l'interconnexion générale début 2006). La technique du « masquerading » permet de cacher un réseau derrière une seule machine passerelle, mais de tels réseaux apparaissent pour le reste d'Internet comme une seule machine.



9 Coment connecter un réseau quand on a une seule adresse IP

Expliquons ici le « masquerading » : une passerelle se fait passer pour toutes les machines du réseau à la fois. La passerelle possède l'adresse IP, les autres machines ont des adresses fictives (typiquement `192.168...`). Ce tour de passe passe est possible grâce aux numéros de ports de TCP qui sont utilisés comme deux octets d'adressage supplémentaires : quand un paquet TCP arrive à la passerelle, celle-ci va transmettre le paquet à l'hôte qui a initié une connexion depuis ce port.

Si plusieurs hôtes utilisent le même port, la passerelle doit jongler avec les numéros de port pour éviter les collisions. Elle peut aussi utiliser l'adresse IP et le port utilisés à l'autre bout de la connexion pour distinguer différentes connexions.

Un routeur Wifi personnel est un exemple typique de passerelle effectuant du « masquerading » pour pouvoir connecter tous les ordinateurs d'une maison à l'internet alors que le fournisseur d'accès n'offre généralement qu'une seule adresse IP.

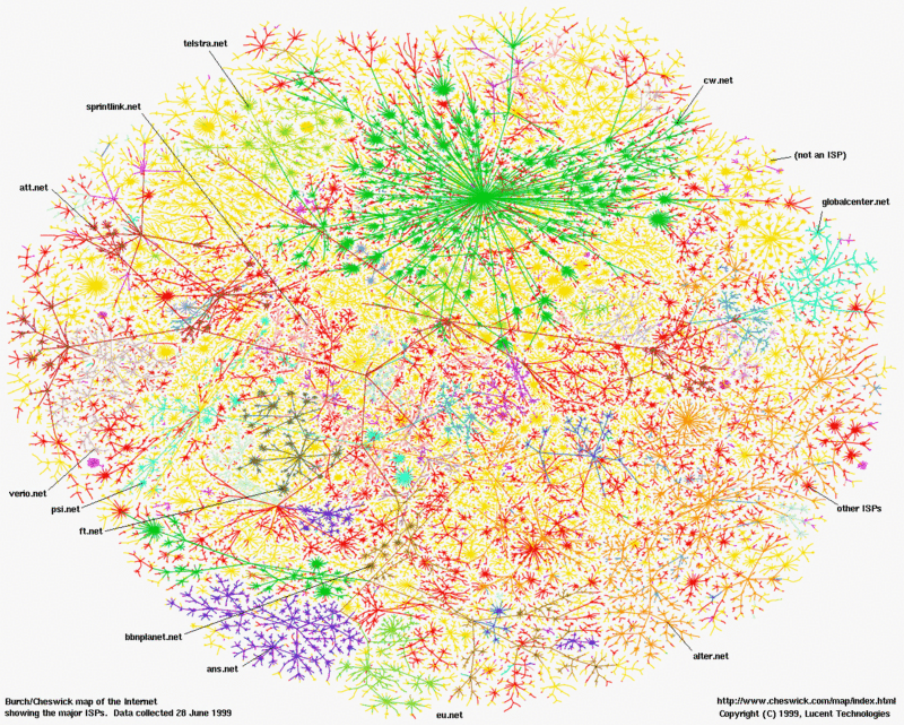
Pour protéger les machines d'un réseau d'attaques, une technique classique consiste à les masquer derrière un pare-feu (ou « firewall » en anglais) qui filtre de plus les paquets entrants ou sortants suspects.

10 IPv6

Avec IP version 4 (IPv4), les adresses sont donc des suites de 32 bits et le nombre d'adresses IP possibles reste limité à 2^{32} soit environ 4 milliards. Malgré plusieurs modifications pour augmenter l'utilisation de l'espace d'adressage (comme la technique du « masquerading » mentionnée ci-dessus), la croissance du nombre d'adresse IP utilisées reste exponentielle. Fatalement viendra un jour où il ne sera plus possible de connecter davantage de réseaux à l'internet par manque d'adresses IP. Ce jour là est déjà anticipé depuis le milieu des années 1990 avec la version 6 de IP (IPv6) qui utilise des adresses de 128 bits, largement de quoi donner une adresse IP à tous les appareils électroniques que la Terre porte ou portera. Cette version d'IP fonctionne en fait déjà sur de nombreux ordinateurs (comme les systèmes unix et en particulier linux et MacOSX) et sur environ un millier des 22 000 systèmes autonomes actuels. Elle est prévue pour cohabiter avec IPv4 de sorte à effectuer une transition progressive.

11 Recherche

Donner une idée de la recherche autour du fonctionnement d'internet. (Conception des protocoles du futurs, intégrations des nouvelles formes de réseaux comme le ad hoc, mesure et modélisation de l'internet.)



12 web

Ne pas confondre l'internet avec la toile qui est le réseau des pages web...

13 DNS

Domain Name Server : l'annuaire de l'internet. Le sytème qui répond l'adresse IP de `interstices.info` est `194.199.19.15`.

14 Pourquoi un tel essor

Ce qui caractérise le plus l'internet est sans doute l'absence d'entité centralisatrice et une architecture ouverte : n'importe qui peut se connecter quelle que soit la technologie utilisée dans son réseau. Les entités qui dirigent chaque réseau décident de se connecter les unes aux autres au grès d'accord bi ou multi-latéraux. Une série de spécifications publiques indiquent les règles à respecter pour pouvoir se connecter. C'est cet aspect ouvert des spécifications qui rend possible le fonctionnement d'un tel conglomérat de réseaux.

15 Liens

On peut inclure dans le texte ci-dessus les liens importants (ceux qui ont un commentaire entre parenthèses).

- internet society
- `http://www.ietf.org/` (Organisme de standardisation de l'internet : voir RFC Pages. Amusant de donner les numéros des RFCs les plus connus : IP :791, TCP :793, DNS :1035, IPv6 :1881, HTTP :1945)

- http://www.isoc.org/

- histoire
- http://fr.wikipedia.org/wiki/Internet
- http://en.wikipedia.org/wiki/Internet
- http://www.zakon.org/robert/internet/timeline/
- http://www.netvalley.com/cgi-bin/intval/net_history.pl?chapter=1
- http://www.isoc.org/internet/history/
- http://www.livinginternet.com/
- http://www.davesite.com/webstation/net-history.shtml

- Louis Pouzin :
- http://www.admi.net/cgi-bin/wiki?LouisPouzin (Louis Pouzin, précurseur méconnu de l'internet)
- http://www.cyclades.com/company/interview.php
- http://www.cs.utexas.edu/users/chris/think/Cyclades/Bibliography/

- host count, mapping (images), cidr
- http://www.isc.org/index.pl?/ops/ds/hosts.php
- http://www.caida.org/ (Mesure d'internet.)
- http://www.caida.org/analysis/topology/as_core_network/AS_Network.xml
- http://www.caida.org/projects/internetatlas/gallery/ches/isp-ss.gif
- http://www.caida.org/outreach/papers/2000/asia_paper/asia_paper.html
- http://www.cidr-report.org/ (Taille d'internet vue par les routeurs BGP des systèmes autonomes.)

- vocabulaire, journal officiel
- http://www.culture.gouv.fr/culture/dglf/cogeter/16-03-99-internet-listes.html (Faut-il écrire « Internet » ou « l'internet » ?)